Cloud.com CloudStack Community Edition 2.1 Beta Installation Guide

July 2010

© 2010 Cloud.com Inc. All rights reserved. Specifications are subject to change without notice. The Cloud.com logo, Cloud.com, Hypervisor Attached Storage, HAS, Hypervisor Aware Network, HAN, and VMSync are trademarks or registered trademarks of Cloud.com, Inc. All other brands or products are trademarks or registered trademarks of their respective holders.

Contents

[1 Overview 4](#_Toc267302483)

[2 Prerequisites 5](#_Toc267302484)

[3 Installing and Setting Up the CloudStack Management Server 6](#_Toc267302485)

[4 Describe Your Deployment 8](#_Toc267302486)

[4.1 Configure the First Zone 8](#_Toc267302487)

[4.2 Using DHCP Provided by the CloudStack (optional) 9](#_Toc267302488)

[4.2.1 Add a Direct IP Address Range 9](#_Toc267302489)

[4.2.2 Configure the CloudStack to Provide DHCP 9](#_Toc267302490)

[4.3 Setting Up Service Offerings (Optional) 9](#_Toc267302491)

[4.4 Setting Up Disk Offering (Optional) 10](#_Toc267302492)

[4.5 Checking the Computing Node 10](#_Toc267302493)

[4.6 Setting up Primary and Secondary Storage Devices 10](#_Toc267302494)

[4.6.1 Primary Storage 10](#_Toc267302495)

[4.6.2 Secondary Storage 11](#_Toc267302496)

[5 Set up the Console Proxy on the Management Server 12](#_Toc267302497)

[6 Installing and Setting Up the CloudStack Agent on a Computing Node 13](#_Toc267302498)

[6.1 Additional Computing Nodes 14](#_Toc267302499)

[7 Testing 15](#_Toc267302500)

[8 Advanced Configuration for Virtual Networking (Optional) 16](#_Toc267302501)

[8.1 Add a Public IP Address Range 16](#_Toc267302502)

[8.2 Add a Virtual Network Service Offering 16](#_Toc267302503)

[9 Troubleshooting 17](#_Toc267302504)

[9.1 cloud-setup-agent Fails 17](#_Toc267302505)

[9.2 Fully Qualified Domain Name 17](#_Toc267302506)

[9.3 Template Download Fails 17](#_Toc267302507)

[9.4 cloud-setup-management Fails 18](#_Toc267302508)

# Overview

Cloud.com CloudStack Version 2.0 is designed to work with a wide variety of enterprise-grade and commodity network and storage infrastructure including the following:

* Layer-3 switching at the core and layer-2 switching at the edge. With layer-3 switching at the core, there is no limit on the number of physical servers that can be managed in a cloud.
* 1-GbE and 10-GbE Ethernet NICs and switches
* NFS and local storage

The CloudStack consists of two types of nodes:

* **CloudStack Management Server**: This server is the resource manager in the system. It controls allocation of virtual machines to Computing Nodes and assigns storage and IP addresses to the virtual machine instances.
* **CloudStack Computing Node**: The Computing Nodes run the virtual machine instances. Servers are grouped into Zones and Pods. The initial installation has one Zone and one Pod.
  + **Zone**: A Zone consists of multiple Pods. Typically a Zone is a datacenter.
  + **Pod**: A Pod is usually one rack of hardware and will include primary storage and a layer-2 switch.

For this release, there is one Management Server and multiple Computing Node servers. The Management Server is installed on an Ubuntu 10.04, Fedora 13, or RHEL/CentOS 5 system that could be a VM or a dedicated server. The CloudStack Agent is installed on the Computing Nodes. Additional Computing Nodes can be added after the initial installation. The Computing Nodes must also be Ubuntu 10.04, Fedora 13, or RHEL/CentOS 5.

**Note: In a single server installation, the Management Server and the Agent may be installed on the same server. The Agent should be installed first, then the Management Server.**

# Prerequisites

The Cloud.com CloudStack has the following hardware and software requirements.

|  |  |  |
| --- | --- | --- |
|  | **Description** | **Minimum Requirements** |
| **Management Server** | Hosts the Cloud.com CloudStack Management Server Software. | * 64-bit x86 CPU (more cores equals better performance) * 2 GB of memory * 80 GB of local disk * At least 1 NIC * Ubuntu 10.04 64-bit, Fedora 13 64-bit, RHEL/CentOS 5 64-bit * Statically allocated IP address * Fully Qualified Domain Name as returned by the hostname command |
| **Computing Node** | Provides all the CPU and memory resource for allocated guest virtual machines. | * 64-bit x86 CPU (max # of cores for better performance) * Hardware virtualization support required * 4 GB of memory * 30 GB of local disk * At least 1 NIC * Ubuntu 10.04 64-bit , Fedora 13 64-bit, RHEL/CentOS 5.5 64-bit * Statically allocated IP Address |

# Installing and Setting Up the CloudStack Management Server

Begin by installing the CloudStack Management Server.

**Note: Make sure that the Management Server has a fully-qualified domain name as returned by “hostname”. For example, “cloud.example.com” is fully qualified, but “cloud” is not. Usually you can correct the lack of a FQDN by editing /etc/hosts.**

**Running NTP is recommended.**

1. Install MySQL. On Ubuntu:

# aptitude install mysql-server

On Fedora and RHEL/CentOS:

# yum install mysql-server

1. Edit the MySQL configuration to suit the CloudStack application. Do this by editing /etc/mysql/my.cnf (on Ubuntu) or /etc/my.cnf (on Fedora and RHEL/CentOS) and inserting the following lines in the [mysqld] section. For example you could place them directly below the datadir line.

innodb\_rollback\_on\_timeout=1

innodb\_lock\_wait\_timeout=600

In Fedora and RHEL/CentOS you will need to start MySQL and enable it on boot:

# service mysqld start

# chkconfig mysqld on

1. Prepare the repository to find the CloudStack packages.

On Ubuntu you will need to edit /etc/apt/sources.list and add:

deb http://download.cloud.com/apt/ubuntu/stable/oss ./

On Fedora you will need to add the CloudStack repo:

cd /etc/yum.repos.d/

wget http://download.cloud.com/foss/fedora/cloud.repo

On RHEL/CentOS you will need to add the CloudStack repo:

cd /etc/yum.repos.d/

wget http://download.cloud.com/foss/centos/cloud.repo

1. Update your local package list and install the CloudStack Console Proxy. On Ubuntu:

# aptitude update

# aptitude install cloud-console-proxy

On Fedora and RHEL/CentOS:

# yum clean all

# yum install cloud-console-proxy

1. Install the management server. On Ubuntu:

# aptitude install cloud-client

On Fedora and RHEL/CentOS:

# yum install cloud-client

1. Set up the database. The CloudStack will connect to the database as the cloud user. Typically it will do the deployment as the root user. Use the first argument set to specify the cloud user password and the --deploy-as option to specify the root user’s password (if set) during database set up.

**Note: This command will fail if the host does not have a fully qualified domain name as returned by the hostname command.**

On Ubuntu the MySQL install prompts for a password. This is the password that you should use in the --deploy-as option. On Ubuntu:

# cloud-setup-databases cloud:<dbpassword> kvm --deploy-as=root:<rootpassword>

On Feodra and RHEL/CentOS MySQL does not prompt for a password on install. The command line below assumes MySQL root does not have a password. If it does you should run the Ubuntu version of this command above. On Fedora and RHEL/CentOS:

# cloud-setup-databases cloud kvm --deploy-as=root

1. Set up the Management Server. This will modify iptables and /etc/sudoers.

# cloud-setup-management

# Describe Your Deployment

Now your CloudStack Management Server is running. The next step is to tell it about the computer nodes, storage, and network configuration that you have done in the previous sections. CloudStack supports networking where the guest VMs are attached directly to the network. They are not NATed as they were in 2.0 beta. The CloudStack can use an externally-provided DHCP server (e.g., one that you manage and run) or a DHCP server managed by the CloudStack.

**NOTE: You should not run two DHCP servers on the same subnet. They will conflict with each other. Most users will want to use externally-provided DHCP.**

To begin describing your deployment, log in to the Administrator Web UI:

http://management-server-ip-address:8080/client

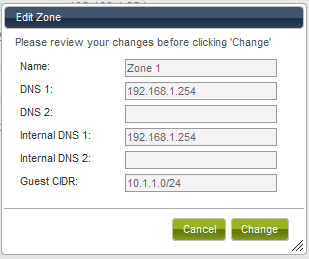
The default user is “admin” and the default password is “password”.

Once you have logged on, see the following sections to set up your Zones and Offerings.

## Configure the First Zone

The CloudStack provides a default Zone. You should edit this Zone to ensure that it has the correct settings for your environment.

1. Click on the Configuration tab.
2. Navigate to the Zones section by clicking on Zones right next to Global Settings.
3. Click on “Default” to show the Default Zone.
4. To edit a Zone click on “Edit Zone” in the lower right of the window.



The CloudStack distinguishes between internal and public DNS. Internal DNS is assumed to be capable of resolving internal-only hostnames, such as your NFS server’s DNS name. Public DNS is provided to the guest VMs for DNS resolution. You can enter the same DNS server for both types. Note that you must provide at least 1 public DNS server and at least 1 Internal DNS server. You will need to provide:

* **Name**: This can be anything to name the Zone.
* **DNS 1 and 2**: These are DNS servers for use by guest VMs in the Zone. These DNS servers will be accessed via the public network you will add later. The public IP addresses you provide for the Zone must have a route to the DNS server named here.
* **Internal DNS 1 and 2**: These are DNS servers for use by system VMs in the Zone. These DNS servers will be accessed via the private network interface of the System VMs. The private IP address you provide for the Pods must have a route to the DNS server named here.
* **Guest CIDR**: Editing this field is an advanced topic that will be discussed in follow-up documentation.

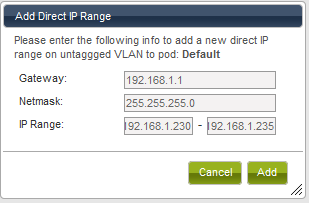
## Using DHCP Provided by the CloudStack (optional)

**This step is required if you would like the CloudStack to provide DHCP services to the guests. Skip to section 4.3 if the guests should use your network's existing DHCP server.**

### Add a Direct IP Address Range

Now add a Direct IP address range. These are the IP addresses that will be assigned to guests when they boot. Typically they are in an RFC 1918 range (e.g., 192.168.3.0/24). Direct IP address ranges are added on the Pod.

Click on the arrow next to the Zone. Then click on the Pod "Default" that appears. Click “Add Direct IP Range” on the right.



This dialog requires the following information:

* **Gateway**:This is the gateway in use for these IPs.
* **Netmask**: This is the netmask associated with this IP range.
* **IP Range**: This takes a lower and an upper IP address that together form a range. These IP addresses will be assigned directly to the guests via DHCP.

Example: The IP address of cloudbr0 is 192.168.1.147. Gateway is 192.168.1.1, and netmask is 255.255.255.0. The IP Range must be unused and continuous, and have at least 2 available IP addresses. An example range is 192.168.1.230 - 192.168.1.235.

### Configure the CloudStack to Provide DHCP

By default the CloudStack does not provide DHCP to the guests. Enable CloudStack DHCP by:

1. Go to the Configuration tab
2. Find the configuration variable direct.attach.network.externalIpAllocator.enabled
3. Click edit on the right of that variable and change its value to false.
4. Restart the Management Server with

# service cloud-management restart

## Setting Up Service Offerings (Optional)

The CloudStack ships with several default service offerings and disk offerings. You can optionally edit these now or proceed with the defaults. The offerings are also in the Configuration tab under Service Offerings, which is next to Zones. This area displays a list of service offerings. Add or edit service offerings as needed. To add a service offering you need to provide:

* **Name**: The name of the service offering.
* **Display text**: A short description of the offering.
* **Storage type**: The type of disk that should be allocated to the guest. Local allocates from storage attached to the KVM Host OS directly. Shared allocates from storage accessible via NFS.
* **Number of CPU cores**: How many cores an instance with this offering should be allocated.
* **CPU (in MHz)**: The CPU speed of the cores that the instance is allocated.
* **Memory (in MB)**: The amount of memory in megabytes that the instance should be allocated.
* **Network Type**: Choose direct.
* **Tags**: an optional comma-delimited list of tags used to match the root disk of guest to primary storage. For example, "fast". See also primary storage below.

The service offering provides CPU and RAM.

## Setting Up Disk Offering (Optional)

You can also edit the Disk Offering. This link is next to the Service Offerings link. The available parameters to add or edit disk offerings are:

* **Name**: Name of the disk offering (e.g. extra large)
* **Description**: A short description of the disk offering
* **Disk size**: The size of the disk offering in GB (e.g. 1 is a 1 GB offering)
* **Tags**: an optional comma-delimited list of tags used to match this disk to primary storage. For example, "fast". See also primary storage below

## Checking the Computing Node

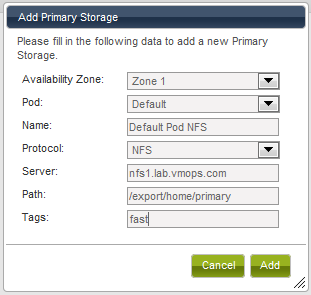
Check to ensure that the Computing Node (the KVM Host) has been recognized by the system. Click on the Hosts tab. You should see this host in the list of available hosts.

## Setting up Primary and Secondary Storage Devices

Next you will need to tell the system about the primary and secondary storage devices that are available. Click on the Storage tab near the top of the UI, and set up each of the following sections.

### Primary Storage

The Primary Storage section will display first. Click on Add Primary Storage. The following dialog will display.



Provide information for the following fields:

* **Availability Zone**: the Zone of the storage device
* **Pod**: the Pod of the storage device
* **Name**: a name to assist you in recognizing the storage device
* **NFS Server**: the DNS name or IP address of the NFS server
* **Path**: the exported path to the storage
* **Tags**: an optional comma-separated list of attributes of the storage device. For example, fast. Service and Disk offerings can have tags as well. A storage allocation succeeds only if there is primary storage that offers all of the tags on the service and disk offering.

### Secondary Storage

You will need to add secondary storage. This process is similar to primary storage. Click on the Secondary Storage link near Primary Storage to begin.

# Set up the Console Proxy on the Management Server

1. Return to the Management Server shell. Set up the CloudStack Console Proxy by running the following command.

# cloud-setup-console-proxy

The CloudStack Console Proxy will ask for the Management Server’s IP address.

# Installing and Setting Up the CloudStack Agent on a Computing Node

Now install the CloudStack Agent on each Computing Node using the following steps. All commands should be run as root. On Fedora you have to make sure that the hostname resolves in DNS or /etc/hosts.

1. Add access to the Cloud.com repository if you have not already done so. On Ubuntu you will need to edit /etc/apt/sources.list and add:

deb http://download.cloud.com/apt/ubuntu/stable/oss ./

On Fedora download the Cloud.com respository:

cd /etc/yum.repos.d/

wget http://download.cloud.com/foss/fedora/cloud.repo

On RHEL/CentOS download the Cloud.com respository:

cd /etc/yum.repos.d/

wget http://download.cloud.com/foss/centos/cloud.repo

1. Update your local package list and install the CloudStack Agent. On Ubuntu:

# aptitude update

# aptitude install cloud-agent

On Fedora and RHEL/CentOS:

# yum clean all

# yum install cloud-agent

1. Disable SELinux . This is usually needed on Fedora and RHEL/CentOS and not needed on Ubuntu.

Set SELinux up to be permissive by default. First, set the SELINUX variable in /etc/selinux/config to “permissive”. This ensures that MySQL and the Management Server can run properly on system reboot. Then set SELinux to permissive until the system is rebooted:

setenforce permissive

1. Set up the CloudStack Agent by running the following command.

# cloud-setup-agent

The CloudStack Agent will ask for the Management Server’s IP address. You will be prompted to enter this during the CloudStack Agent setup. You may see some failure messages when stopping services in this script; that is fine.

If you have multiple Pods configured you will be prompted to select which Pod this Compute Node should join. Select the appropriate Pod.

**Note: A Computing Node must have a statically allocated IP address; the cloud-agent-setup will error and fail if a dynamically-assigned address is present.**

**A Computing Node’s host OS must also have a fully qualified domain name. Usually you can correct the lack of a FQDN by editing /etc/hosts. You will also want to make sure that the IP address associated with the hostname is the IP address of the default route table entry (usually eth0). If the hostname resolves to 127.0.0.1 guest networking will not work.**

1. Open up the iptables ports to allow console proxy access and allow bridge traffic to pass to the guests. Alternatively you can disable the User Firewall (on Ubuntu) or stop the iptables service (Fedora, RHEL/CentOS).

On Ubuntu:

# iptables -I FORWARD -i cloudbr0 -o cloudbr0 -j ACCEPT

# ufw allow proto tcp from any to any port 5900:6100

Edit /etc/ufw/before.rules and place the following above the COMMIT line

-I ufw-before-forward -i cloudbr0 -o cloudbr0 -j ACCEPT

On RHEL/CentOS:

# iptables -I INPUT -i cloud0 -j ACCEPT

# iptables -I FORWARD -i cloud0 -o cloud0 -j ACCEPT

# iptables -I FORWARD -i cloudbr0 -o cloudbr0 -j ACCEPT

# iptables –I INPUT -m tcp -p tcp --dport 5900:6100 –j ACCEPT

Then save your new iptables rules:

# service iptables save

On Fedora:

# iptables -I FORWARD -i cloudbr0 -o cloudbr0 -j ACCEPT

# iptables –I INPUT -m tcp -p tcp --dport 5900:6100 –j ACCEPT

Then save your new iptables rules:

# service iptables save

The CloudStack Agent is now installed and set up.

## Additional Computing Nodes

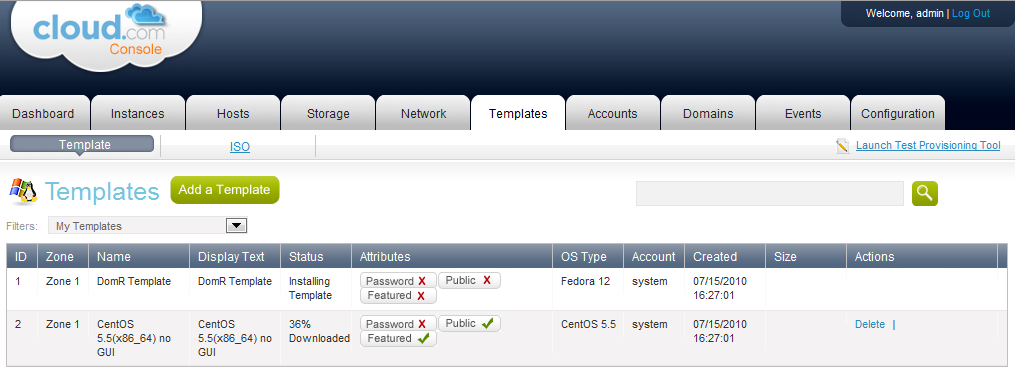
You can add additional Computing Nodes to your CloudStack cloud. Repeat Step 5 on each KVM-enabled Computing Node that you would like to add to the cloud. Once installed and configured the Agent will automatically connect to the Management Server.

# Testing

When secondary storage is available the Management Server will begin downloading the two provided templates. These templates are large and may take 10–20 minutes to download depending on the speed of your network.

**Important: If you attempt to start virtual machines prior to the completion of the download of both templates the VM creation will fail.**

The UI provides a progress indication for the provided CentOS template in the Templates tab. You can click “Refresh” on the lower, right side of the page to update the download percentage. When that download completes you can begin using the system.



Try creating a new virtual machine. Go to the Instances tab and click on “Create a new VM” and follow the wizard steps. It may take several minutes to start the first VM. Subsequent VM starts should be faster. Once the CentOS image is up the root password is “password”. You can use the console viewer (from the Instances tab) to log in.

You can create additional users and administrators for the system. Click on the “Launch Test Provisioning Tool” on the upper right of the screen to do this.

You may want to read the Administration Guide available at <http://open.cloud.com>.

# Advanced Configuration for Virtual Networking (Optional)

The CloudStack supports virtual networking as discussed earlier. Virtual networking is enabled by adding Public IP addresses to the CloudStack.

## Add a Public IP Address Range

Go to the Configuration tab and select a Zone. Select "Add Public IP Range". These are the IP addresses that will be assigned to accounts when a public IP address is requested. Usually they are routable from the external intranet, but you can use a RFC 1918 range (e.g., 192.168.3.0/24) if needed.

This dialog requires the following information:

* **Gateway**:This is the gateway in use for these IP’s.
* **Netmask**: This is the netmask associated with this IP range.
* **IP Range**: This takes a lower and an upper IP address that together form a range. These IP addresses are assumed to be accessible from the public internet and will be allocated for access to guest networks.

Example: The IP address of cloudbr0 is 192.168.1.147. Gateway is 192.168.1.1, and netmask is 255.255.255.0. The IP Range must be unused and continuous, and have at least 2 available IP addresses. An example range is 192.168.1.150 - 192.168.1.159.

## Add a Virtual Network Service Offering

Add a Service Offering to support virtual networking. See section 5.3. For network type, choose "virtual" instead of direct.

# Troubleshooting

## cloud-setup-agent Fails

cloud-setup-agent may fail with the error message “KVM needs to be enabled”. That is usually caused by the absence of KVM in the kernel. You can add KVM to the kernel with the following steps:

# modprobe kvm

Then you will need to execute one of the two following commands. If the machine has an Intel CPU:

# modprobe kvm\_intel

Or if the machine has an AMD CPU:

# modprobe kvm\_amd

## Fully Qualified Domain Name

Cloud-setup-databases will not run if the host does not have a fully qualified hostname. Usually there are two things you need to do to fix this.

Check the output of “hostname”. It will show something like “foo”. You need to run it again to add your domain name to it:

# hostname foo.example.org

Then you should edit /etc/hosts. Make sure that your fully qualified hostname resolves to the IP address on eth0.

## Template Download Fails

The template download can fail for a variety of reasons. One common problem is that there is a required HTTP proxy. The CloudStack does not currently support outbound HTTP access via a proxy. To circumvent this you can download the template manually and then use a provided script to load the template into the CloudStack. To do this:

Manually download the two templates into a local directory. You will need to retrieve [http://download.cloud.com/templates/builtin/a88232bf-6a18-38e7-aeee-c1702725079f.qcow2.bz2](http://download.vmops.com/templates/builtin/a88232bf-6a18-38e7-aeee-c1702725079f.qcow2.bz2) and [http://download.cloud.com/templates/builtin/eec2209b-9875-3c8d-92be-c001bd8a0faf.qcow2.bz2](http://download.vmops.com/templates/builtin/eec2209b-9875-3c8d-92be-c001bd8a0faf.qcow2.bz2). In the example below we assume the local directory is /root/templates.

Now mount secondary storage to /root/secondary. For example,

# mount –t nfs nfsserver:/export/home/cloud/secondary /root/secondary

Load the template with

# /usr/lib64/cloud/agent/scripts/storage/qcow2/importmpl.sh -m /root/secondary -r /root/templates/a88232bf-6a18-38e7-aeee-c1702725079f.qcow2.bz2 -v /root/templates/eec2209b-9875-3c8d-92be-c001bd8a0faf.qcow2.bz2

And then unmount secondary storage with

# umount /root/secondary

## cloud-setup-management Fails

If cloud-setup-management fails like this:

# cloud-setup-management

Welcome to the CloudStack Management setup

hostname.company.com

The hostname of this machine is properly set up

Executing the following reconfiguration script:

ins spec after /files/etc/sudoers/spec[last()]

set /files/etc/sudoers/spec[last()]/user cloud

set /files/etc/sudoers/spec[last()]/host\_group/host ALL

set /files/etc/sudoers/spec[last()]/host\_group/command ALL

set /files/etc/sudoers/spec[last()]/host\_group/command/tag NOPASSWD

save

Saving failed

error: No match for path expression

sudoers reconfiguration failed

CloudStack Management Server setup aborted

Then you need to update Augeas to at least version 0.7.1:

# yum update augeas